

The principles and practices within Data Security, Governance and Compliance and their implementation into a company.

Matthew Cragg

Cyber Security and Networking (of MSc Year 1)

Data Security, Governance and Compliance

University of Wales Trinity St. Davids

Swansea, Wales

Student ID: 2207432

CONTENTS

I	Introduction	1
II	Research	2
II-A	Acts and Compliances	2
II-B	Security Models	2
II-B1	ISO 27000	2
II-B2	NIST SP 800-53	2
II-B3	Which to use?	2
III	Security, Governance and Compliance.	2
IV	Security	2
IV-A	Networks	2
IV-B	VLANs	4
V	Conclusion	4
VI	Terminology	4
VII	Reference List	5

LIST OF FIGURES

1	An assumed model of current topology used within CoffeeBlend.	3
2	An assumed model of current topology used within CoffeeBlend, with three additional customers connected.	3
3	A screenshot of the router settings currently in place within a CoffeeBlend store.	3
4	Proposal of the suggested topology that is recommended to be used within a CoffeeBlend store.	3

LIST OF TABLES

I	Table demonstrating the various VLANs and available IPs that should be used for CoffeeBlend employees.	4
----------	--	---

Abstract—The consistent evolution of security merits constant changes within the law and acts created to protect the information and data of customers. As the threat of cyber security attacks increase with the growth of a company, it is paramount that the company combats these threats within the confinements of the law and data acts. While CoffeeBlend prides itself on one of the most sought-after coffee blends in the world, it's security and policies are nothing to be proud about.

I. INTRODUCTION

Traditionally, security has always been viewed by the average person as how secure the padlock on a door is. However, as data and customer information moves away from filing cabinets and towards being stored online on a server, new measures must be taken to ensure that the data is safe and secure. Consequently, new laws and data acts are required to be created and introduced to further protect customers and employees. While these laws change depending on the country and continent that the company is based in, it is still important to be mindful of the physical location of each store. According to the website Pensar.co.uk on the topic of GDPR regulations, [1] 'As of May 2018, any business interacting with EU customer data needs to protect the data by the same standards'.

This necessitates that companies keep track of where their stores are based, and what laws each store must abide to. The main aim of the General Data Protection Regulation, or GDPR act of 2018 is, according to Privacy Trust, [2] 'provide a set of standardized data protection laws across all the member countries'. This should allow members of the EU to track and understand where and how their data is being used.

In relation to CoffeeBlend, assuming that some of their stores are built within the EU, then any data held and gathered by the company should be noted and expressed to the customer. This involves data as simple as what type of coffee a customer purchases on a regular basis, to their name, gender and phone number. The GDRP also expresses the right to allow any customer to see and delete their data at any given time, at their request. Despite the complications of Brexit, the UK is still expected to follow GDRP regulations, Therefore any UK

based CoffeeBlend stores are required to follow suit with the acts.

II. RESEARCH

A. Acts and Compliances

As mentioned already, the company would be required to abide by the GDPR policy assuming that some of the companies building's are based within the UK and other EU countries. While the United States of America lacks their own version of GDPR at the time of writing, a similar policy is in place in the state of California called the California Consumer Privacy Act, or CCPA.

Within the UK, there exists a regulation designed specifically for the sale of coffee. Named "The Coffee and Coffee Regulations 1987" act. It exists to ensure that customers know exactly what they are drinking. For example, part 5.b discusses the use of the word 'decaffeinated', and when it is acceptable to use it. This act also requires a company to hold a Food Hygiene Rating certificate, which is given based on how clean and how the company prepares food.

B. Security Models

A security framework is a generic blueprint offered to companies to use as an outline for the creation of their InfoSec environment. A framework is a broad set of guidelines that is designed to set up an entire environment. Alternatively, a security model is a blueprint offered by a security organisation and is used for a specific item. An example of a security model is the 2FA, or Two Factor Authentication, service offered by [3] Cisco called 'Duo'. This service is bought by a company and then implemented by Cisco once the contract has been put in place.

1) *ISO 27000*: One of the most widely used security models within businesses is the International Organisation for Standardization, ISO 27000. According to the authors of the article 'Integrated installing ISO 9000 and ISO 27000 management systems on an organisation', [4] 'ISO 27000 might effectively facilitate the implementation and maintenance of multiple management systems'. The security model itself is split into two main sections. Section one of the ISO 27000 security model details documentation and how to integrate a document management system framework into a business. Section Two of the model discusses various suggested practices of implementing integrated management systems.

2) *NIST SP 800-53*: Another popular security framework is one developed by NIST, who are known for creating an extensive library of IT standards throughout the years they have been active. According to the website Techtarget.com [5] 'NIST SP 800-53 is the security benchmark for US government agencies'. This has spurred NIST SP 800-53 to be used very widely within the private sector.

3) *Which to use?*: While both security frameworks offer a wide range of guidance and support, neither ISO 27000 or NIST SP 800-53 is necessarily 'better' than the other. In a high-level comparison written by Prameet P. Roy, they examine both frameworks in extreme detail and compare the

positives and negatives of both. However, the concluding verdict states [6] 'Instead of choosing one framework over the other, the best approach would be to combine the best practices and points of both'. The reasoning behind the authors choice is that modern day risk assessment is no trivial task. Attackers in the modern age have state-of-the-art tools and software, and are often more innovative than any companies defence can prepare for. Therefore, it is usually beneficial to take the best parts of both framework that is relevant to your company.

III. SECURITY, GOVERNANCE AND COMPLIANCE.

For CoffeeBlend, a unique set of policies, frameworks and laws must be abided. Within the UK, they must ensure that each of the following are implemented properly and abided.

- GDPR.
- BYOD.
- The Coffee and Coffee Products Regulation of 1987.
- Service Level Agreement.
- Contingency Plan.
- Risk Assessment.

Failure to do could result in either a large fine, prison sentence and/or termination of the company, depending on the severity. As laws, guidelines and acts are constantly changing and being updated, it is paramount that a company of CoffeeBlend's size keeps track of any potential changes and adapts accordingly.

Contingency planning is an important part of risk management and assessment. It ensures that if something was to go wrong with the company, such as a financial crash for example, then there is a motion in place ready to go to protect both staff and customers.

Risk assessment is an important aspect of ensuring a company continues to operate smoothly. Examples include checking the surrounding areas of a potential new store to be built, that the product will actually make a profit. CoffeeBlend will need to keep this in mind when opening new stores and hiring new staff. Because the intellectual properties owned by CoffeeBlend are incredibly valuable, security precautions should be taken to ensure that the properties are probably secured and protected.

A service level agreement will need to be signed between CoffeeBlend and their suppliers. This is a contract that documents and creates a list of everything that CoffeeBlend will be purchasing. Once a service level agreement has been written, signed and approved, here will always be a level of services agreed upon, and therefore expected. This will be useful if a supplier is not delivering the goods expected, as this agreement can be used in a court of law.

IV. SECURITY

A. Networks

Figure 1, page 3 is the assumed current network in place at a standard CoffeeBlend store. The first immediate flaw is the lack of Firewalls in place. There is no form of security between the employee workstations and the internet.

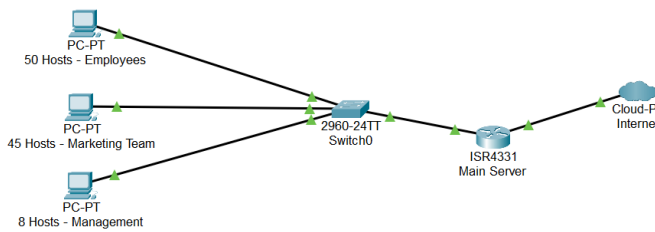


Fig. 1. An assumed model of current topology used within CoffeeBlend.

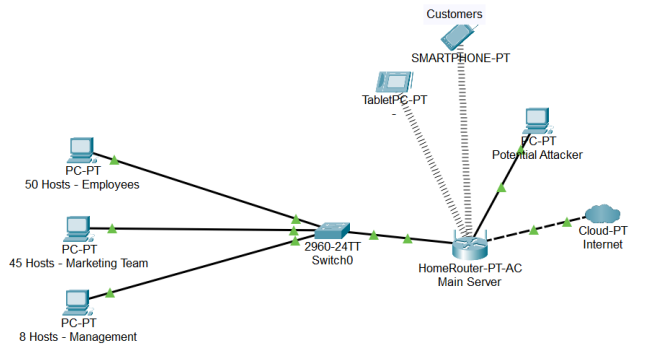


Fig. 2. An assumed model of current topology used within CoffeeBlend, with three additional customers connected.

Within figure 2, page 3, three customers have accessed the guest network. While the guest network is separate to the main network that the employees are directly connected to, this is still not enough to offer protection to employee and customer data. In some coffee stores, there are exposed ethernet ports. While these can be useful for some customers who wish for faster internet speeds than what wireless can offer, it is a risk for the company store if the network is not configured properly.

Management	
Router Access	Router Password: ●●● Re-enter to confirm: ●●●
Router Information	
Firmware Version:	v0.9.7
Current Time:	Not Available
Firewall	
SPI Firewall Protection: ☐ Enabled ☐ Disabled	
Wireless Security	
☒ Allow guests to see each other and access the local network	

Fig. 3. A screenshot of the router settings currently in place within a CoffeeBlend store.

Looking at the router settings above within the store, displayed within figure 3, page 3 there are a number of security risks immediately noticeable. The password is only three letters long, which could easily be guessed as '123' or 'ABC'. It would also not take a password cracker application such as Cain and Abel very long to break. Once an attacker

has successfully changed the router password, they are free to do as they please within the network.

While the firmware version is kept up-to-date, the current time of the router has not been synced with either a server or master router. While this seems like a minor issue, having the correct time synced to a router is important for logging purposes, and to know when a setting was changed. Therefore, if there was an attack and someone was able to access the network, having the correct time on the router will show when exactly the attack took place.

The Firewall has been disabled on the router. The Firewall is a device that focuses on security, and monitors all incoming and outgoing traffic. If there are any unrecognised bytes of data, or 'Packets', the Firewall can block them and keep the channels open. The Firewall can be configured to only allow specific types of data, so any unknown or illegal types of data (Like videos, if YouTube is banned for employees for example).

The final important risk on the router is that guests can see other guest devices on the network. This is a risk because attackers are able to access and compromise other customer devices, which would violate GDPR as CoffeeBlend would be risking customer data and information.

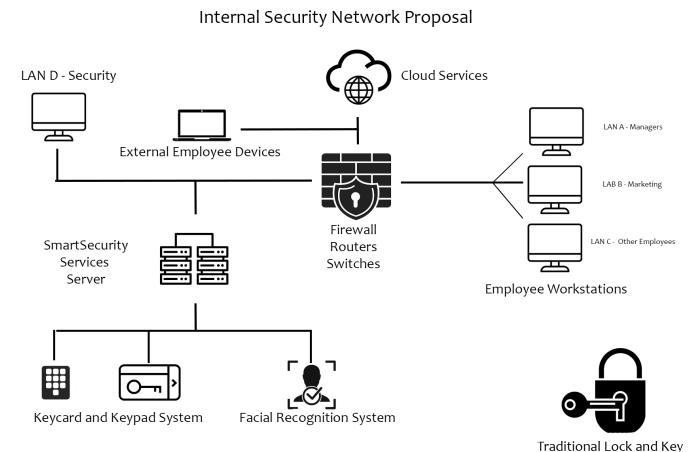


Fig. 4. Proposal of the suggested topology that is recommended to be used within a CoffeeBlend store.

Figure 4, page 3 displays the recommended internal employee network for CoffeeBlend. At the top of the diagram, the Cloud Network offers a direct connection to the external employee devices that they may bring in. This will allow employees to continue to use their own workstations or use mobile phones during breaks, without allowing them full access to the network. This policy is known as Bring Your Own Device, or commonly known as the acronym BYOD. This policy, according to NCSC.gov.uk, this concept has only been recently adopted due to the recent COVID-19 pandemic, but has seen considerable use since, and any company wishing to allow employees to bring their own device must [7] 'determine what approach will best suit your organisation's. In the situation CoffeeBlend finds itself in, the pressure by both the

employees and customers to use their own devices warrant the use of BYOD, and must develop the network system accordingly. The customers, for example, should never be on the same network that hosts the same systems that control the security to the building, or the customer data that is stored, whereas it would be acceptable to allow the employees to be on the same network as their work.

Therefore, the following diagram proposes another network that would be for external use only, and would allow customers to use the internet without the risk of a customer accessing the companies records or data. This isolation would be paramount, as any risk of a customer being able to access the companies information would result in severe consequences.

The three main security components are the key card, keypad, and facial recognition software, all are connected to the SmartSecurity Services server. The only computer able to access this server is the security computer, which has also been isolated on its own VLAN. This ensures that no one else is able to access the security server and change crucial settings, such as opening doors to non-employees. A new security team will required to help facilitate and create these changes.

The isolated lock and key is not part of the network, yet is still considered security. Therefore, it still finds a place on the diagram.

B. VLANs

The computers connected to the network have been isolated into their own VLANs, or Virtual Local Area Networks. These are used to segregate the traffic from the subnetted workstations. While this also helps with ensuring the right amount of traffic and bandwidth is reserved for the right amount of workstations, it also prevents users from each VLAN to see traffic and data transmitted and received in another VLAN. For example, the employees within VLAN B, the marketing team, cannot see the traffic coming to and from VLAN A, which is reserved for the managers workstations.

The following has been made with the assumption that there are 118 employees in total at this one CoffeeBlend site, consisting of fifty staff, forty marketing members, twenty security team members and eight management. Each VLAN can be subnetted, meaning that only a certain amount of IPs can be reserved for each VLAN. This would allow only a controlled amount of people to access the VLAN, and no more. Assuming that the companies IP is 192.168.20.0/24, and if the company only wanted four VLANs, it could be separated into the following.

Within table I, page 4 shows that there are sixty-four IP addresses reserved for VLAN A, which is for the bulk of employees. This means that will be enough IP addresses for the fifty current employees, and fourteen extra IP addresses that will be unused, and can be reserved for any additional staff that may be hired in the future. The marketing team similarly has another sixty-four IP addresses reserved in VLAN B, for the current forty-five employees and room for expansion. The security team in VLAN C has only twenty IP addresses available, one for each host. This is important because it means

Amount of Hosts	VLAN A	VLAN B	VLAN C	VLAN D
Other Employees 50 Hosts	192.168.20.1/26 to 192.168.20.63/26			
Marketing Team 45 Hosts		192.168.20.64/26 to 192.168.20.127/26		
Security 20 Hosts			192.168.20.129/27 to 192.168.20.159/27	
Management 8 Hosts				192.168.20.160/30 to 182.168.20.168/30

TABLE I

TABLE DEMONSTRATING THE VARIOUS VLANS AND AVAILABLE IPs THAT SHOULD BE USED FOR COFFEEBLEND EMPLOYEES.

no one else is able to enter the VLAN C without first removing a member of staff or host machine from the VLAN, which would consequently raise concerns and alert the IT team that something is wrong. In VLAN D, the management team only has eight IP addresses, which is reserved for each of the eight host machines that the managers use. This also means that only managers may use this VLAN, with no threat of unauthorised access on this network. If an employee wishes to bring in their own device to work, they must abide by the Bring Your Own Device policy discussed earlier, and they will be forced to use the employee-only network that connects directly to the Cloud, and not the building's server unless authorised. If a VLAN is not currently using all available IP addresses, the unused addresses may be blocked, preventing any unwanted persons to access the system and claim the IP. When a new employee joins a specific time, the IP may be unblocked and therefore assigned to the new employee.

V. CONCLUSION

Based upon the report, we can conclude that CoffeeBlend requires a significant restructuring in policies, law and guidelines. All employees must be informed of the new changes, and key cards, codes and IP addresses all need to be assigned per employee, as stated within the internal employee network proposal. The new security team will need to be informed of all policies and compliances, as they will be the ones within each store expected to uphold and maintain them. While all of these changes and improvements will be of significant cost, it will be beneficial to ensure that the company is legal and operating as a modern company.

If CoffeeBlend implements all of these changes, then their company policies, compliances and security will be something something else to be proud of.

VI. TERMINOLOGY

List of terminologies used in this document:-

- RAM - Random Access Memory.
- GDPR - General Data Protection Regulation.
- VLAN - Virtual Local Area Network.
- IP - Internet Protocol.
- InfoSec - Information Security.

VII. REFERENCE LIST

- [1] M. Williams, “Data protection in the US vs Europe: what businesses need to know.” [Online]. Available: <https://www.pensar.co.uk/blog/data-protection-in-the-us-vs-europe>
- [2] “Whats the real purpose of the GDPR?” [Online]. Available: <https://www.privacytrust.com/gdpr/whats-the-real-purpose-of-the-gdpr.html>
- [3] “Two-Factor Authentication (2FA).” [Online]. Available: <https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa>
- [4] C.-H. Wang and D.-R. Tsai, “Integrated installing iso 9000 and iso 27000 management systems on an organization,” in *43rd Annual 2009 International Carnahan Conference on Security Technology*, 2009, pp. 265–267.
- [5] “Top 10 IT security frameworks and standards explained.” [Online]. Available: <https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one>
- [6] P. P. Roy, “A high-level comparison between the nist cyber security framework and the iso 27001 information security standard,” in *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTE)*, 2020, pp. 1–3.
- [7] “Bring your own device (BYOD).” [Online]. Available: <https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device>